This listing of claims will replace all prior versions, and listings, of claims in the application:

IN THE CLAIMS

1. (Currently Amended). A secure architecture for preventing copying of digital content by way of a computing platform, the secure architecture comprising:

a secure computing platform for receiving and storing encrypted or encoded digital content from the Internet and from a remote source of digital content as well as storing local encrypted or encoded data, and processing said encrypted or encoded digital data, said computing platform including a host processor and a peripheral bus, said computing platform configured to run audio or video playback application software for passing said encrypted or encoded digital data to said peripheral bus,

a playback device ~~configured to be connected to said computing platform for receiving encrypted or encoded digital content from said computing platform by way of said peripheral bus~~ ~~, said playback device~~ including a separate ~~processor,~~ content processor and a peripheral bus interface for receiving said encrypted or encoded digital content from said peripheral bus, ~~in said computing platform and~~ said ~~separate~~ content processor configured to decrypt and decode ~~decrypting or decoding~~ said encrypted or encoded digital content and control playback of said digital content by said playback device , said playback device also including a memory device for storing decoding or decryption software, ~~said peripheral interface coupled to said peripheral bus for receiving said encrypted and encoded digital signals from said peripheral bus,~~ said playback device configured to decrypt or decode said encrypted or encoded digital data and generate a decoded or decrypted output signal for playback, said playback device configured so that ~~computing platform cannot access~~ said decrypted or decoded digital content is inaccessible by said computing platform when said playback device is connected to said computing platform.

2. (Previously Presented). The secure architecture as recited in claim 1, wherein said computing platform includes a network interface for receiving digital data from an external network.

3. (Previously Presented). The secure architecture as recited in claim 1, wherein said peripheral bus is a USB bus.

4. (Currently Amended). The secure architecture as recited in claim 1, wherein said p(New)eripheral peripheral bus is a PCI bus.

5. (Previously Presented). The secure architecture as recited in claim 1, wherein said peripheral bus is a Fire Wire bus.

6. (Previously Presented). The secure architecture as recited in claim 1, further including one or more user input devices.

7. (Previously Presented). The secure architecture as recited in claim 1, wherein said computing architecture includes one or more local persistent storage devices.

8. (Currently Amended)   A secure hardware architecture for preventing copying of digital content by way of a computing platform, the secure architecture   comprising:

a computing platform for receiving and storing encrypted or encoded digital content from the Internet as well as storing local encrypted or encoded data, and processing said encrypted or encoded digital data, said computing platform including a host processor and a peripheral bus, said computing platform configured to run audio or video playback application software for passing said encrypted or encoded digital data to said peripheral bus, said computing platform configured so that said peripheral bus is not accessible by said audio or video playback software running on said computing platform;

a playback device configured to be connected to said computing platform for receiving encrypted or encoded digital content from said computing platform, said playback device including a separate content processor, and a peripheral bus interface for receiving said encrypted or encoded digital signals content from said peripheral bus, and said content processor decrypting or decoding configured to decrypt or decode said encrypted or encoded digital content data signals, said playback device also including a local memory device for storing decoding or decryption software, said peripheral interface coupled to said peripheral bus for receiving said encrypted and encoded digital signals from said peripheral bus, said playback

3

~~device configured to decrypt or decode said encrypted or encoded digital data and~~ said content processor also configured ~~generate a decoded or decrypted analog output signal for playback~~ ~~wherein said playback device is configured~~ to create a list of decrypted or decoded digital content stored on said playback device, wherein playback device is configured so that said decrypted and decoded digital content is inaccessible by said computing platform when said computing platform is connected to said playback device.

9. (Previously Presented) The secure architecture as recited in claim 8, wherein said playback device is further configured to enable editing of said list.